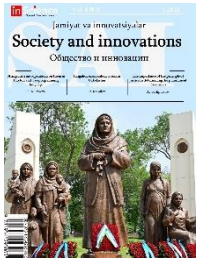
Жамият ва инновациялар –
Общество и инновации –
Society and innovations
Journal home page:
https://inscience.uz/index.php/socinov/index




# Prospects for legal policy in the field of combating cybercrime in Uzbekistan

**Abdulaziz RASULEV**[1]

Institute of Legislation and Legal Policy under the President of the Republic of Uzbekistan

**ARTICLE INFO**

***Article history:***
Received April 2023
Received in revised form
15 May 2023
Accepted 15 June 2023
Available online
25 June 2023

***Keywords:***
cybercrime,
cybersecurity,
legal policy,
information technology,
criminal legislation,
preventative measures,
scientific research,
virtual space,
international cooperation,
digitalization.

**ABSTRACT**

This article addresses the issue of cybercrime and the need to counter this phenomenon in the Republic of Uzbekistan. The author highlights the inadequacy of existing criminal legislation in the field of cybersecurity and its lack of conformity with the requirements of modern information technologies. Several cases of hacking government and information resources in Uzbekistan are mentioned, emphasizing the importance of taking preventive measures. The article proposes conducting scientific research, implementing specialized prevention strategies, and fostering a culture of behavior in the virtual space. It also emphasizes the importance of strengthening international cooperation in the field of cybersecurity. The main goal of the proposed legal policy is to ensure the effective protection of individuals, society, and the state in the era of digitalization and the development of the digital economy.

2181-1415/© 2023 in Science LLC.
DOI: https://doi.org/10.47689/2181-1415-vol4-iss3-pp124-132


# O‘zbekistonda kiberhujumlarga qarshi kurash sohasidagi huquqiy siyosat istiqbollari

***Kalit so‘zlar:***
kiberjinoyat,
kiberxavfsizlik,
huquqiy siyosat,
axborot texnologiyalari,
jinoiy qonunchilik,
profilaktika chora-tadbirlari,
ilmiy tadqiqotlar,
virtual makon,

**ANNOTATSIYA**

Ushbu maqolada kiberjinoyat muammosi va O‘zbekiston Respublikasida ushbu hodisaga qarshi kurashish zarurligini ko‘rib chiqiladi. Muallif kiberxavfsizlik sohasida mavjud jinoiy qonunchilikning yetishmovchiligini va uning axborot texnologiyalarining zamonaviy voqeliklari talablariga mos kelmasligini qayd etadi. Muallif shuningdek, Ozbekistondagi davlat va axborot resurslarining buzib kirilgan bir qator holarni

[1] Doctor of Law, Professor, Scientific Secretary, Institute of Legislation and Legal Policy under the President of the Republic of Uzbekistan

xalqaro hamkorlik, raqamlashtirish.

ta'kidlab, uning oldini olish chora-tadbirlarini ko'rish zarurligini qayd etadi. Ilmiy tadqiqotlar, maxsus profilaktika chora-tadbirlari olib borish va virtual makonda xulq madaniyatini shakllantirish, shuningdek, kiberlxavfsizlik sohasida xalqaro hamkorlikni kuchaytirish tavsiya qilinadi.

# Перспективы правовой политики в области противодействия киберпреступности в Узбекистане

***Ключевые слова:*** киберпреступность, кибербезопасность, правовая политика, информационные технологии, уголовное законодательство, профилактические меры, научные исследования, виртуальное пространство, международное сотрудничество, цифровизация.

**АННОТАЦИЯ**

В данной статье рассматривается проблема киберпреступности и необходимость противодействия этому явлению в Республике Узбекистан. Автор указывает на недостаточность существующего уголовного законодательства в области кибербезопасности и несоответствие его требованиям современных реалий информационных технологий. Основная цель правовой политики – обеспечить эффективную защиту личности, общества и государства в эпоху цифровизации и развития цифровой экономики.

Ни для кого не секрет, что будущее и прогресс сегодня определяется своевременным развитием и внедрением современных технологий. Интернет стал важной платформой в нашей жизни. Согласно данным Международного Статистического портала на начало 2023 года **5,16 миллиардов** людей или **64,4 % населения** Земли составляют пользователи Интернета, что и подтверждает тезис о том, что мы практически не можем представить свою жизнь без виртуального пространства.

Рекордный темп роста числа пользователей сети в Узбекистане наблюдался в последние десять лет. Их количество увеличилось с 16 % до 86 % населения. Согласно данным Министерства цифровых технологий Республики Узбекистан количество пользователей всемирной сети превысило **31 миллион человек**.

Цифровые технологии, искусственный интеллект, криптоэкономика и другие стали основным катализатором глобализации. Не зря ООН назвала цифровые технологии как «эффективное средство достижения всех 17 целей в области устойчивого развития». Глобальное развитие с использованием цифровых технологий поэтому и называют **цифровым будущим**.

К сожалению, есть обратная сторона монеты. Современные технологии стали использоваться злоумышленниками ради достижения преступных целей. Возник феномен киберпреступности, который по своим масштабам и степени общественной опасности намного опережает традиционную преступность.

Согласно данным экспертно-аналитической компании ASTRA в 2022 году ущерб от киберпреступности составил около **6 триллионов долларов США**! Это больше, чем ВВП Японии, Германии, Индии, Великобритании и Франции.

Между тем, предполагаемый ущерб к 2025 году составит **10,5 триллионов долларов США**. Для сравнения, этот прогнозируемый показатель превышает ВВП всех стран мира, кроме Китая и США, равен **10 % мирового ВВП**.

По данным ФБР каждый день происходит около **2328 киберпреступлений**, о которых потерпевшие могут и не знать. Университет Мэриленда провел исследование и выявил, что каждые 39 секунд происходит хакерская атака. За последние 20 лет 80% зарегистрированных киберпреступлений, как правило, связаны с фишинговыми атаками. Фишинг, как мы знаем, это вид несанкционированного доступа к конфиденциальной информации. При этом цель такого доступа может быть разной. Поэтому киберпреступность может наносит вред отдельному человеку, так и транснациональным компаниям, государству в целом.

Почему нужна правовая политика? Именно слаженная работа государства, в первую очередь, судов и правоохранительных органов позволит эффективно противодействовать угрозам киберпреступности, координировать усилия и средства. Кроме того, правовая политика будет воплощена в надлежащем законодательстве, мерах профилактики.

**Основная сущность правовой политики в области противодействия киберпреступности в Республике Узбекистан**

Правовая политика Республики Узбекистан в области противодействия киберпреступности направлена на создание эффективного механизма выявления и расследования этих преступлений, привлечение виновных к ответственности, а также защиту интересов личности, общества и государства в виртуальном и цифровом пространстве.

В статье 54 новой редакции Конституции прямо указывается, что **обеспечение прав и свобод человека — высшая цель государства**. Поэтому правовая политика в сфере противодействия киберпреступности должна быть направлена именно на защиту прав и свобод человека в киберпространстве.

В своем выступлении на расширенном заседании Совета безопасности от 13.01.2023 года Ш.Мирзиёев отметил, что «**в условиях нынешних напряженных геополитических противостояний обостряются проблемы в экономической, социальной, политической сферах, информационной безопасности и других областях**». Действительно, обеспечение информационной безопасности является одним из способов противодействия киберпреступности.

Правовая политика Узбекистан в этом направлении активно формировалась в последние 10-15 лет, а в последние 2-3 года проходит этап последовательной трансформации.

В целом сущность правовой политики в области противодействия киберпреступлениям в Республике Узбекистан выражается в следующем:

1. ***Законодательное закрепление защиты интересов личности, общества и государства в информационной сфере***. Закон Республики Узбекистан от 12 декабря 2002 года № 439-II «О принципах и гарантиях свободы информации» закрепил понятия **информационной безопасности**, поделив ее на информационную безопасность личности, общества и государства. Так государственная политика в этой сфере направлена на

предотвращение угроз безопасности личности, общества и государства в информационной сфере;

недопущение противоправного информационно-психологического воздействия на общественное сознание, манипулирования им;

защиту информации, а также государственных секретов и государственных информационных ресурсов от несанкционированного доступа к ним.

2. ***Установление ответственности за преступления в сфере информационных технологий.*** Уголовный кодекс Республики Узбекистан, который был принят первым среди стран СНГ, предусматривал ответственность за нарушение правил информатизации. В 2007 году государство усилило ответственность за совершение незаконных действий в области информатизации и передачи данных. Была введена отдельная глава XX1 – Преступления в сфере информационных технологий. Эта глава предусматривает **семь составов** преступлений:

Кроме того, предусматривается более строгая ответственность за совершение **13 составов** преступлений с использованием информационных технологий.

Сейчас данная сфере также трансформируется. В Концепции совершенствования уголовного и уголовно-процессуального законодательства Республики Узбекистан, утвержденной постановлением Президента Республики Узбекистан от 14 мая 2018 года № ПП–3723, в рамках обеспечения действенной и надежной охраны прав и свобод граждан, интересов общества и государства была указана необходимость **пересмотра норм, предусматривающих ответственность в сфере информационных технологий с учетом технологического прогресса**, **в том числе расширение категорий преступлений, связанных с киберпреступностью**. В связи с этим разрабатывается проект УК в новой редакции, где нормы в этой сфере планируется совершенствовать.

На наш взгляд при создании раздела новой редакции УК о киберпреступности следует учитывать, что согласно Закону Республики Узбекистан «О кибербезопасности» **киберпреступность** означает *совокупность преступлений, осуществляемых в киберпространстве с использованием программного обеспечения и технических средств, с целью завладения информацией, ее изменения, уничтожения или взлома информационных систем и ресурсов.*

Значит юридический анализ киберпреступности предполагает: объект – безопасность киберпространства; объективная сторона – неправомерные действия в виде завладения, изменения, уничтожения или взлома информационных систем и ресурсов; место совершения преступления – киберпространство; орудие и средства совершения преступления – программное обеспечение и технические средства; субъективная сторона – умысел, цель – специальная; субъект – физическое лицо, достигшее возраста уголовной ответственности.

3. ***Создание организационно-технических основ противодействия преступлениям в сфере информационных технологий***. Постановлением Президента Республики Узбекистан от 14 сентября 2019 года № ПП–4452 ГУП было создано ГУП «**Центр кибербезопасности**», находящееся в ведении **Службы государственной безопасности** Республики Узбекистан. Уполномоченным

органом в сфере регулирования кибербезопасности была определена Служба государственной безопасности Республики Узбекистан.

Так, Центр кибербезопасности осуществляет сбор, анализ и накопление данных о современных угрозах информационной безопасности, выработку рекомендаций и предложений по оперативному принятию эффективных организационных и программно-технических решений, обеспечивающих предотвращение актов незаконного проникновения в информационные системы, ресурсы и базы данных государственных органов и организаций.

Кроме того, Центр взаимодействует с операторами и провайдерами сетей телекоммуникаций, правоохранительными органами в рамках проведения анализа, идентификации нарушителей, методов и средств, используемых при осуществлении несанкционированных либо деструктивных действий в информационном пространстве.

В целях своевременного оповещения национальных пользователей сети Интернет о возникающих угрозах информационной безопасности в национальном сегменте сети Интернет ежегодно центр публикует итоговый отчет о кибербезопасности в Узбекистане. В отчете можно увидеть проблемы и рекомендации по минимизации рисков при использовании современных технологий.

В свою очередь, применяются меры по защите банковского сектора от киберугроз. Создан и функционирует **Центр обнаружения, предотвращения и расследования компьютерных атак в банковской сфере при Центральном банке Республики Узбекистан.**

4. ***Реализация мер по цифровизации. Противодействие преступности в сфере цифровых технологий не препятствует развитию этих технологий в различных отраслях Республики Узбекистан***. Так в 2020 году Указом Президента Республики Узбекистан № УП–6079 была принята **Стратегия** «**Цифровой Узбекистан – 2030**». Благодаря имплементации этой стратегии начата реализация свыше 220 приоритетных проектов, предусматривающих совершенствование системы электронного правительства, дальнейшее развитие отечественного рынка программных продуктов и информационных технологий, организацию во всех регионах республики IT-парков, обеспечение данной сферы квалифицированными кадрами.

**Приоритетные направления совершенствования правовой политики в области противодействия киберпреступлениям в Республике Узбекистан**

**Первое направление** – совершенствование уголовного законодательства Республики Узбекистан. На наш взгляд, проблемы противодействия преступлениям в сфере цифровых технологий в Республике Узбекистан могут быть эффективно решены лишь при наличии соответствующего и отвечающего требованиям времени уголовного законодательства. Здесь можно выделить несколько проблем, требующих решения.

Во-первых, слабая гармонизация норм УК Республики Узбекистан в части ответственности за киберпреступления нормам законодательства в сфере информационных технологий и безопасности.

Следует отметить, что нормы некоторых этих нормативно-правовых актов не нашли свое подкрепление в части ответственности в КоАО или УК Республики Узбекистан. Так, несмотря на потенциальную опасность и угрозу сети Интернет

для молодежи ответственность за распространение среди детей негативной информации, наносящей вред их здоровью, согласно Закону Республики Узбекистан «О защите детей от информации, наносящей вред их здоровью» не предусмотрена. Аналогично в действующем законодательстве отсутствует специальная правовая норма, устанавливающая ответственность блогера за нарушение требований Закона Республики Узбекистан «Об информатизации».

Во-вторых, недостаточная имплементация норм международного права.

Международные акты в этой сфере определяют противодействие нарушениям конституционных (личных) прав и свобод личности в информационных системах и глобальной сети Интернет; защита частной собственности в информационной среде, противодействие киберпиратству, нарушающему авторские и смежные права собственников и товарных знаков; противодействие изготовлению, распространению негативного контента в информационном пространстве государства; защиту информационно-коммуникационных технологий и инфраструктуры от негативного внешнего воздействия; противодействие информационным войнам; борьбу с кибертерроризмом. Эти нормы могут быть использованы в совершенствовании норм УК Республики Узбекистан. Например, Решение Совета Евросоюза от 28 мая 2001 года «Противодействие мошенничеству и подделке безналичных средств оплаты» (2001/413/JHA) указывают на криминализацию мошеннических действий, совершенных в виртуальном пространстве. С учетом схожести хищений в виртуальном пространстве предлагается объединить все киберхищения в единую статью. Договор ВОИС по авторскому праву требует осуществления эффективных действий против любого акта нарушения прав, включая срочные меры по предотвращению нарушений, и меры, являющиеся сдерживающим средством от дальнейших нарушений авторов, что может быть использовано для совершенствования статьи 149 УК Республики Узбекистан.

В-третьих, использование устаревшего понятийного аппарата в структурировании диспозиции статей УК Республики Узбекистан, обобщенность объекта уголовно-правовой охраны киберпреступлений.

Следует отметить, что по действующему УК Республики Узбекистан преступления в сфере информационных технологий указаны в разделе преступления против общественной безопасности и общественного порядка. Однако киберпреступления могут наносить вред не только общественной безопасности, но и безопасности личности или государства. Поэтому указанный родовой объект является недостаточно точным.

Определенная проблема возникает и при квалификации преступлений в этой сфере с учетом терминологии. Так статьи 2781-2787 используют понятия компьютера, электронно-вычислительных машин, в то время как эти понятия не соответствуют современным реалиям динамики развития преступлений в сфере информационных технологий и безопасности. Так не представляется возможным определить мобильное устройство в качестве компьютера. То же самое можно указать про компьютерную информацию.

В-четвертых, Несоответствие действующей главы XX1 УК Республики Узбекистан современным вызовам и угрозам кибербезопасности.

Действующая редакция главы XX1 УК Республики Узбекистан не предусматривает четкое подразделение статей объекту уголовно-правовой

охраны. В свою очередь, отсутствие ответственности за нарушение требований размещения информации в сети Интернет, несанкционированный доступ к компьютерной информации, составляющей охраняемую законом тайну, не позволяет обеспечить принцип неотвратимости ответственности.

Если сравнивать санкции норм УК, то можно увидеть огромную разницу. Так максимальное наказание за компьютерный саботаж независимо от вреда – составляет три года лишения свободы. Максимальное наказание за незаконный оборот продукции, получаемой из семян хлопчатника, составляет десять лет лишения свободы. На наш взгляд, компьютерный саботаж, то есть вывод из строя важнейшей стратегической системы имеет большую общественную опасность, чем незаконная продажа продуктов, получаемых из семян хлопчатника.

Исходя из динамики развития и «арены» совершения преступлений в сфере информационных технологий и коммуникаций предлагается включить в УК Республики Узбекистан концептуально новый раздел «Киберпреступления», предусматривающий три главы – 1) преступления против информационной безопасности; 2) преступления в сфере телекоммуникаций и связи; 3) преступления против безопасности стратегической информационной инфраструктуры.

В этих главах следует установить ответственность за такие киберпреступления, как нарушение законодательства о защите детей от информации, наносящей вред их здоровью; нарушение требований размещения информации в сети Интернет; преследование или травля в виртуальном пространстве (кибербуллинг, кибersталкинг); киберпиратство (нарушение прав интеллектуальной собственности в Интернете); кибертерроризм (выведение из строя или атаки на стратегические объекты).

**Второе направление** – усиление организационно-технического обеспечения кибербезопасности. Отчет «Центра кибербезопаности» свидетельствует о наличии угроз в сфере обеспечения кибербезопасности.

Так, в 2021 году Центром было выявлено более 17 миллионов случаев вредоносной и подозрительной активности в национальном сегменте сети Интернет, 76 процентов из них – бот-сети. Именно бот-сети используются киберпреступниками для заражения вредоносными программами и контроля за цифровыми технологиями в качестве большой зомби-сети.

Также является неудовлетворительным то, что из 38000 активных доменов лишь 14014 были защищенными. То есть 63 % национальных доменов были незащищенными. Такого рода проблемы стали таковыми из-за использования ненадлежащих программных средств, мер безопасности.

К сожалению, пользователи не обращают внимание на важность экспертизы ресурсов на соответствие требованиям кибербезопасности. В связи с этим в рамках правовой политики государству следует принять меры для того, чтобы сделать экспертизу информационных систем на предмет соответствия кибербезопасности привлекательной. Аналогично и с сертификацией систем менеджмента информационной безопасности. Необходимо обсудить вопрос о порядке обязательной сертификации и экспертизы информационных ресурсов, имеющих критическое значение.

Третье направление – принятие мер по профилактике и предупреждению киберпреступлений. К сожалению, противодействие киберпреступлениям, в

основном, сводится к борьбе с последствиями уже совершенного преступления. Так называемая «работа» с потенциальными правонарушителями не ведется на должном уровне. Осбенно сейчас необходимо обратить внимание на формирование личности хакеров. В частности, использование цифровых технологий в так называемых в информационных войнах превращают их в самых опасных преступников. Так, Лига безопасного интернета обнаружила около 2900 фейков о событиях в Казахстане в начале января 2022 года, что подрывает информационную безопасность. Все мы Хакеры из знаменитой хакерской группировки Anonymous объявили «кибервойну» правительству России в связи с военной операцией в Украине. Такое положение дел явно меняет представление о хакерах как о простых взломщиков. Сейчас хакеры – это своеобразные «солдаты», которые могут вести войну в киберпространстве. Не зря, видимо, на пороге XXI в. один американский генерал заявлял: «Дайте мне с десяток хакеров, и я поставлю на колени любую страну».

Вызывают глубокую озабоченность и действия хакеров в Узбекистане. К примеру, в мае 2012 года хакеры группировки «Clon Securuty», которая предположительно включает представителей из Узбекистана и других стран Центральной Азии, взломали сайт Минздрава Узбекистана с призывом недопущения стерилизации матерей.

20 февраля 2013 года эта же группировка взломала сайт МВД Кыргызской Республики.

19 ноября 2013 года хакерская группировка Bangladesh Grey Hat Hackers взломала веб-сайты газеты «Народное слово» и ее узбекской версии «Халқ сўзи». Аналогичный случай с республиканской газетой имел место и 27 марта 2016 года.

25 июля 2020 года атака была осуществлена на сайт Агентства по противодействию коррупции Республики Узбекистан, которое обвинялось хакерами предположительно за отказ в приеме на работу.

Аналогичный взлом «недовольного» с результатами собеседования для приема на работу хакера группировки «Clon Securuty» был осуществлен в отношении сайта хокимията Сурхандарьинской области 6 января 2021 года.

Атака на сайт IT-парка от 26 мая 2021 года, когда на главной странице была демонстрирована игра «Сапер», свидетельствует о хулиганских мотивах хакеров. Подобного рода атаки свидетельствуют об уязвимости государственных информационных ресурсов, в связи с чем предупреждение подобных случаев требует адекватного реагирования со стороны законодателя.

Недавний февральский репортаж UzReport о хакер из Узбекистана, который украл из банков Швейцарии, Бельгии, Польши, Южной Кореи и Израиля более $50 млн долларов, также свидетельствует о важности профилактических мер. За это он был приговорен к восьми годам лишения свободы. По словам парня, первое его дело было, когда он снял $15,2 млн. Также он украл $35 млн из банка Израиля, после чего перевел деньги в банки семи государств, дабы скрыть следы. Безнаказанность и отсутствие профилактических мер способствовали продолжению преступной деятельности.

Руководитель ближневосточного исследовательского центра «Лаборатории Касперского» Амин Хасбини указал, что Узбекистан вошел в число стран, которые чаще всего атакуют хакеры с начала 2023 года. Это и показывает важность

профилактики киберпреступности и обеспечения кибербезопасности для Узбекистана.

В этой связи, правовая политика должна быть направлена на:

- проведение научных и социологических исследований для принятия мер по профилактике и предупреждению правонарушений с использованием современных технологий;

- проведение мер специальной профилактики правонарушений в киберпространстве (в частности, среди лиц, совершивших незначительные правонарушения с использованием современных технологий, ради недопущения повторной и более опасной преступной деятельности);

- формирование культуры поведения и этики в виртуальном пространстве, привитие чувства ответственности за неправомерное использование современных технологий, особенно у молодежи (так, предлагается принять Государственную программу по формированию интернет-культуры, включающий в себя комплекс мер – проведение тренингов, специальных курсов в образовательных учреждениях, подготовку и распространение в СМИ и Интернете пропагандистских материалов (флаеров, стендов, презентаций).

В целом, правовая политика Республики Узбекистан в области противодействия преступлениям в сфере цифровых технологий должна быть направлена на эффективную защиту личности, общества и государства в эпоху цифровизации, обеспечение благополучия и процветания цифровой экономики страны.

**БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ:**

1. un.org/ru/un75/impact-digital-technologies
2. https://www.getastra.com/blog/security-audit/cyber-crime-statistics/
3. https://cybersecurityventures.com/
4. https://basetop.ru/rejting-ekonomik-mira-2021-tablitsa-vvp-stran-mira/
5. Расулев, А. "Противодействие кибертерроризму: международно-правовые и уголовно-правовые аспекты." Review of law sciences 4 (2018): 92-95.
6. Расулев, А. К. "Совершенствование уголовно-правовых и криминологических мер борьбы с преступлениями в сфере информационных технологий и безопасности. д. ю. н.... дис." (2018): 16-18.
7. Расулев, Абдулазиз, and Сурайё Рахмонова. "Преступления в сфере информационных технологий и безопасности: детерминанты и предупреждение." Общество и инновации 1.1 (2020): 200-209.